Family list
2 family member for:
JP11219340
Derived from 1 application.

1 **DEVICE AND SYSTEM FOR AUTHENTICATION MANAGEMENT**
Publication info: **JP3587045B2 B2** - 2004-11-10
JP11219340 A - 1999-08-10

Data supplied from the ***esp@cenet*** database - Worldwide

THIS PAGE BLANK (USPTO)

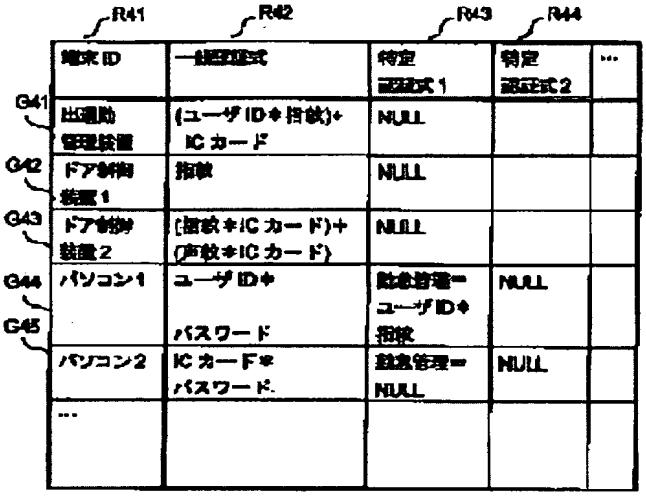
DEVICE AND SYSTEM FOR AUTHENTICATION MANAGEMENT

Patent number: JP11219340
Publication date: 1999-08-10
Inventor: FUJII TERUKO; NAKAMURA HIROSHI; SADAKANE TETSUO; BABA YOSHIMASA
Applicant: MITSUBISHI ELECTRIC CORP
Classification:
- international: G06F15/00
- european:
Application number: JP19980023042 19980204
Priority number(s): JP19980023042 19980204

Report a data error here

Abstract of **JP11219340**

PROBLEM TO BE SOLVED: To enable an administrator to freely set and consistently manage a security policy extending over plural authenticating means by providing a terminal information data base wherein information corresponding to authentication conditions that the plural authenticating means are optionally combined, is registered. SOLUTION: A terminal ID as an identifier indicating a terminal unequivocally is registered in a column R41 of the data structure of authentication conditions, that authenticating means of a terminal information data base are optionally combined and general authentication expressions showing the authentication conditions used for normal authentication for every terminals are registered in a column R42. Further, specific authentication expressions showing authentication conditions exclusive to a specific service and application are registered in columns R43 to R44. Thus, the authentication conditions used for the normal authentication and the authentication conditions used for the specific service and application are registered terminal by terminal distinctively in the terminal information data base and managed by an authentication management device.



Data supplied from the ***esp@cenet*** database - Worldwide

THIS PAGE BLANK (USPTO)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－219340

(43)公開日　平成11年(1999)８月10日

(51)Int.Cl.[6]	識別記号	Ｆ Ｉ	
Ｇ０６Ｆ　15/00	３３０	Ｃ０６Ｆ　15/00	３３０Ａ

審査請求　未請求　請求項の数８　ＯＬ　（全 16 頁）

(21)出願番号　特願平10－23042

(22)出願日　平成10年(1998)２月４日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　藤井　照子
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(72)発明者　中村　浩
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(72)発明者　貞包　哲男
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(74)代理人　弁理士　宮田　金雄　（外２名）

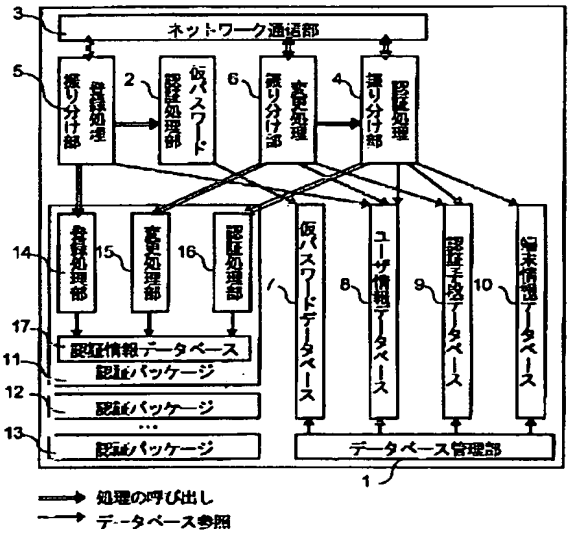
最終頁に続く

(54)【発明の名称】　認証管理装置及び認証管理システム

(57)【要約】

【課題】　管理者が複数の認証手段に跨るセキュリティ・ポリシーを自由に設定し、一貫して管理することができると共に、不正な認証情報の登録を回避して高度なセキュリティを必要とする場合にも適用でき、通常の認証と認証情報変更時の認証とを区別できる認証管理装置及び認証管理システムを得る。

【解決手段】　１又は複数の認証情報を入力する複数の端末とネットワークを介して接続され、複数の端末の認証を管理するものであって、認証管理装置は、少なくとも、複数の端末に入力される認証情報に応じて認証処理を行う１又は複数の認証手段と、ユーザの認証情報に対応する情報が登録されるユーザ情報データベースと、認証手段に対応する情報が登録される認証手段データベースと、認証手段を任意に組み合わせた認証条件に対応する情報が登録される端末情報データベースとを備える。



【特許請求の範囲】
【請求項１】　１又は複数の認証情報を入力する複数の端末とネットワークを介して接続され、上記複数の端末の認証を管理する認証管理装置において、少なくとも、上記複数の端末に入力される認証情報に応じて認証処理を行う１又は複数の認証手段と、上記ユーザの認証情報に対応する情報が登録されるユーザ情報データベースと、上記認証手段に対応する情報が登録される認証手段データベースと、上記認証手段を任意に組み合わせた認証条件に対応する情報が登録される端末情報データベースとを備えることを特徴とする認証管理装置。
【請求項２】　ユーザの上記認証情報を登録する際に参照される仮パスワードと当該仮パスワードの有効期限とを関連付けて登録される仮パスワードデータベースを備え、上記有効期限に応じて又は上記認証情報の登録に応じて上記仮パスワードデーターベースから上記仮パスワードを削除することを特徴とする請求項１に記載の認証管理装置。
【請求項３】　上記認証手段データベースには、通常の認証で用いる一般認証時のしきい値と上記認証情報を変更する際に用いる認証情報変更時のしきい値とを区別して登録でき、上記認証手段は通常の認証には上記一般認証時のしきい値を用い、上記認証情報を変更する際には上記認証情報変更時のしきい値を用いて認証処理することを特徴とする請求項１又は請求項２に記載の認証管理装置。
【請求項４】　上記１又は複数の認証情報の少なくとも一つはバイオメトリクスの認証情報であることを特徴とする請求項１、請求項２又は請求項３に記載の認証管理装置。
【請求項５】　１又は複数の認証情報を入力する複数の端末とネットワークを介して接続され、上記複数の端末の認証を管理する認証管理装置を有する認証管理システムにおいて、上記認証管理装置は、少なくとも、上記複数の端末に入力される認証情報に応じて認証処理を行う１又は複数の認証手段と、上記ユーザの認証情報に対応する情報が登録されるユーザ情報データベースと、上記認証手段に対応する情報が登録される認証手段データベースと、上記認証手段を任意に組み合わせた認証条件に対応する情報が登録される端末情報データベースとを備えることを特徴とする認証管理システム。
【請求項６】　ユーザの上記認証情報を登録する際に参照される仮パスワードと当該仮パスワードの有効期限とを関連付けて登録される仮パスワードデータベースを備え、上記有効期限に応じて又は上記認証情報の登録に応じて上記仮パスワードデーターベースから上記仮パスワードを削除することを特徴とする請求項５に記載の認証管理システム。
【請求項７】　上記認証手段データベースには、通常の認証で用いる一般認証時のしきい値と上記認証情報を変更する際に用いる認証情報変更時のしきい値とを区別して登録でき、上記認証手段は通常の認証には上記一般認証時のしきい値を用い、上記認証情報を変更する際には上記認証情報変更時のしきい値を用いて認証処理することを特徴とする請求項５又は請求項６に記載の認証管理システム。
【請求項８】　上記１又は複数の認証情報の少なくとも一つはバイオメトリクスの認証情報であることを特徴とする請求項５、請求項６又は請求項７に記載の認証管理システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、複数のシステムや端末の認証を管理する認証管理装置及びその認証管理装置を有する認証管理システムに関するものであり、例えば、ネットワークに展開される複数のシステムや端末のバイオメトリクス情報、パスワード等による個人認証を管理する認証管理装置及びその認証管理装置を有する認証管理システムに関するものである。
【０００２】
【従来の技術】情報化社会の発達は、これまで利便性の追求の方向に進んできたが、インターネットの急速な普及は、セキュリティの向上を必要としている。コンピュータ社会におけるセキュリティの構成要素の１つが個人認証である。すなわち、情報やサービスを適切なユーザに対して与えためには、そのユーザが誰であるかを確認することが必須であり、これを行うのが個人認証である。
【０００３】従来からコンピュータシステムによる認証は、様々な場面で行われている。例えば、出退勤管理にはパンチカードに代わってＩＣカードが用いられているし、また、セキュリティの高い部屋のドアの開閉にもＩＣカードや磁気カードが用いられている。また、コンピュータ端末による各種サービスへのアクセスにはパスワードが多用されている。
【０００４】しかし、パスワードは比較的第三者に漏洩しやすく、高度なセキュリティを必要とする場合での適用に問題があった。これに対して近年では、各種技術の進歩に伴い、指紋や声紋等のバイオメトリクス情報を用いた照合やワンタイムパスワード等、様々な認証手段が提案され、実用化されている。
【０００５】例えば、従来のバイオメトリクス情報を用いた認証方法として、特開平８－１６７８８号公報に開示された個人固有の複数の身体的特徴を用いる個人認証方法がある。この方法は、音声、指紋、筆跡等の個人固有の複数の特徴を読み取り、読み取った特徴パラメータをそれぞれ個人の特徴を反映する複数のカテゴリに分割し、分割した各カテゴリをその個人の特徴の現れ易さにより、重み付けを施して統合する。そして、統合により得られた各特徴パラメータをその個人の特徴の現れ易さ

により、重み付けを施して統合し、統合結果をしきい値と比較して本人確認を行う。

【０００６】また、図１４は、従来のバイオメトリクス情報を用いた認証機能を持つ一般的なサービス・サーバの構成を示すブロック図である。図中、サービス処理部３１は、システムの主体となるサービスの処理を行う。例えば、出退勤管理システムでは出退勤管理の処理を行う。認証処理部３２は、バイオメトリクス情報を用いた認証を行う。認証情報データベース３３は、認証に用いられるバイオメトリクス情報を登録する。登録サービス処理部３４は、バイオメトリクス情報を登録するための処理を行う。

【０００７】次に動作について説明する。サービス・サーバに接続された端末からサービスの要求がある場合は、端末からバイオメトリクス情報と共にサービス要求信号が送信される。例えば、指紋情報と共に出退勤管理の要求信号が送信される。これらの情報を受け取ると、サービス処理部３１は認証処理部３２に認証処理を依頼する。認証処理部３２は、端末から送信されたバイオメトリクス情報と認証情報データベース３３に登録されているバイオメトリクス情報とを照合して認証ＯＫか認証ＮＧかを判定し、判定結果をサービス処理部３１に通知する。サービス処理部３１は通知された判定結果に従って、認証ＯＫならサービスを実施し、認証ＮＧならエラーを端末に通知してサービス要求に対する処理を終了する。

【０００８】また、サービス・サーバに接続された端末からバイオメトリクス情報の登録要求がある場合は、端末からパスワードと共に登録要求信号が送信される。この情報を受け取ると登録サービス処理部３４は、まず、パスワードのチェックを行う。その結果がＯＫなら、端末に対してバイオメトリクス情報の送信を要求する。その後、端末からバイオメトリクス情報が送信されると、登録サービス処理部３４は、送信されたバイオメトリクス情報を認証情報データベース３３に登録して登録要求に対する処理を終了する。

【０００９】

【発明が解決しようとする課題】しかしながら従来の認証管理は、様々な条件の下で行われる様々な認証手段の認証を個々に管理するものであるため、管理者が複数の認証手段に跨るセキュリティ・ポリシーを自由に設定し、一貫して管理することができないという問題があった。セキュリティ・ポリシーとは、すなわち、使い勝手やシチュエーションに応じたセキュリティの強度に対する管理者の設計思想や運営についての考え方である。

【００１０】また、例えばバイオメトリクス等の認証情報を登録する際には、パスワードを使用していたが、このパスワードは恒常的に有効であるため、このパスワードが漏洩した場合にはいつでも不正な認証情報を登録される可能性が有り、高度なセキュリティを必要とする場合での適用に問題があった。

【００１１】また、登録されている認証情報を変更する際には、先に述べたパスワードを使用したり、その時点で登録されている認証情報を使用していたが、パスワードを使用する場合には、認証情報の登録の際と同様の問題があった。

【００１２】さらに、登録されている認証情報を変更する際にその時点で登録されている認証情報を使用する場合には、通常の認証と認証情報を変更するための認証との区別がないため、より厳しいセキュリティが必要となる後者のセキュリティを特別に高くすることができないという問題があった。

【００１３】この発明は上記のような問題点を解決するためになされたもので、管理者が複数の認証手段に跨るセキュリティ・ポリシーを自由に設定し、一貫して管理することができると共に、不正な認証情報の登録を回避して高度なセキュリティを必要とする場合にも適用でき、さらに、通常の認証と認証情報変更時の認証とを区別できる認証管理装置及び認証管理システムを得ることを目的とする。

【００１４】

【課題を解決するための手段】この発明に係る認証管理装置は、１又は複数の認証情報を入力する複数の端末とネットワークを介して接続され、複数の端末の認証を管理するものであって、少なくとも、複数の端末に入力される認証情報に応じて認証処理を行う１又は複数の認証手段と、ユーザの認証情報に対応する情報が登録されるユーザ情報データベースと、認証手段に対応する情報が登録される認証手段データベースと、認証手段を任意に組み合わせた認証条件に対応する情報が登録される端末情報データベースとを備えるものである。

【００１５】また、次の発明に係る認証管理装置は、ユーザの認証情報を登録する際に参照される仮パスワードとその仮パスワードの有効期限とを関連付けて登録される仮パスワードデータベースを備え、有効期限に応じて又は認証情報の登録に応じて仮パスワードデーターベースから仮パスワードを削除するものである。

【００１６】また、次の発明に係る認証管理装置は、認証手段データベースに通常の認証で用いる一般認証時のしきい値と認証情報を変更する際に用いる認証情報変更時のしきい値とを区別して登録でき、認証手段は通常の認証には一般認証時のしきい値を用い、認証情報を変更する際には認証情報変更時のしきい値を用いて認証処理するものである。

【００１７】また、次の発明に係る認証管理装置は、１又は複数の認証情報の少なくとも一つはバイオメトリクスの認証情報であるものである。

【００１８】さらにまた、この発明に係る認証管理システムは、１又は複数の認証情報を入力する複数の端末とネットワークを介して接続され、複数の端末の認証を管

理する認証管理装置を有するものであって、認証管理装置は、少なくとも、複数の端末に入力される認証情報に応じて認証処理を行う１又は複数の認証手段と、ユーザの認証情報に対応する情報が登録されるユーザ情報データベースと、認証手段に対応する情報が登録される認証手段データベースと、認証手段を任意に組み合わせた認証条件に対応する情報が登録される端末情報データベースとを備えるものである。

【００１９】また、次の発明に係る認証管理システムは、ユーザの認証情報を登録する際に参照される仮パスワードとその仮パスワードの有効期限とを関連付けて登録される仮パスワードデータベースを備え、有効期限に応じて又は認証情報の登録に応じて仮パスワードデーターベースから仮パスワードを削除するものである。

【００２０】また、次の発明に係る認証管理システムは、認証手段データベースに通常の認証で用いる一般認証時のしきい値と認証情報を変更する際に用いる認証情報変更時のしきい値とを区別して登録でき、認証手段は通常の認証には一般認証時のしきい値を用い、認証情報を変更する際には認証情報変更時のしきい値を用いて認証処理するものである。

【００２１】また、次の発明に係る認証管理システムは、１又は複数の認証情報の少なくとも一つはバイオメトリクスの認証情報であるものである。

【００２２】

【発明の実施の形態】実施の形態１．以下、本発明の認証管理システム及び認証管理装置に係る実施の形態１を説明する。図２に、本発明に係る認証管理システムの構成を示す。図中、認証管理装置２１は、本発明の認証管理装置に相当し、複数の端末の認証を管理する認証管理装置である。端末２２～２４は、認証管理装置２１からの認証管理に応じて各々のサービスをユーザに提供すると共に認証情報を入力する端末である。インタフェース装置２５～２７は、ユーザの認証情報を採取するマン・マシン・インタフェース装置である。ネットワーク２８は、認証管理装置２１と端末２２～２４間の通信を可能とするための通信ネットワークである。

【００２３】また、図３に、この認証管理システムの一具体例を示す。図中、認証管理装置Ａ１は、図２における認証管理装置２１に相当する。出退勤管理装置Ｃ１、ドア制御装置Ｃ２～Ｃ３、勤怠管理装置Ｃ４、メールサーバＣ５は、それぞれ図２における端末２２～２４に相当する。テンキーパットＩ１、指紋取得装置Ｉ２～Ｉ６、ＩＣカードリーダＩ７～Ｉ９、声紋取得装置Ｉ１０、パソコンＩ１１～Ｉ１５は、それぞれ図２におけるインタフェース装置２５～２７に相当する。

【００２４】出退勤管理装置Ｃ１は出退勤を管理すると共にテンキー、指紋及びＩＣ信号の認証情報を入力する装置であり、テンキーパットＩ１、指紋取得装置Ｉ２、ＩＣカードリーダＩ７が接続される。ドア制御装置Ｃ２は比較的セキュリティの低い部屋へのドアを制御すると共に指紋の認証情報を入力する装置であり、指紋取得装置Ｉ３が接続される。ドア制御装置Ｃ３はセキュリティの高い部屋へのドアを制御すると共に指紋、声紋及びＩＣ信号の認証情報を入力する装置であり、指紋取得装置Ｉ４、声紋取得装置Ｉ１０、ＩＣカードリーダＩ８が接続される。

【００２５】勤怠管理サーバＣ４は勤務状況を管理するサーバであり、指紋取得装置Ｉ５～Ｉ６が接続され、指紋の認証情報を入力するパソコンＩ１１～Ｉ１２が接続される。メールサーバＣ５はメールの送受信を管理するサーバであり、ＩＣ信号の認証情報を入力するものを含むパソコンＩ１１～Ｉ１５が接続される。

【００２６】テンキーパットＩ１は、ユーザが０から９の１０種類の数字を入力できるマン・マシン・インタフェース装置である。指紋取得装置Ｉ２～Ｉ６は、ユーザの指紋を読み取り、デジタルデータに加工するマン・マシン・インタフェース装置である。ＩＣカードリーダＩ７～Ｉ９は、ＩＣカード内の認証情報を読み出すマン・マシン・インタフェース装置である。声紋取得装置Ｉ１０は、ユーザの声紋を取得し、デジタルデータに加工するマン・マシン・インタフェース装置である。パソコンＩ１１～Ｉ１２は、指紋取得装置Ｉ５～Ｉ６が接続されたパソコンである。パソコンＩ１３～Ｉ１４は、通常のパソコンである。パソコンＩ１５は、ＩＣカードリーダＩ９が接続されたパソコンである。

【００２７】図３において、例えば、ユーザが出退勤管理装置Ｃ１のサービスを利用する場合、ユーザはテンキーパットＩ１、指紋取得装置Ｉ２などを用いて認証用の認証情報を出退勤管理装置Ｃ１に入力しする。これに応じて、出退勤管理装置Ｃ１は入力された認証情報と共に認証コマンドをネットワークを介して認証管理装置Ａ１に送信する。その後、認証管理装置Ａ１は受信した情報に基づいて認証を行い、認証結果をネットワークを介して出退勤管理装置Ｃ１に送信する。そして、出退勤管理装置Ｃ１は認証結果に基づいて、認証ＯＫの場合に、出退勤のデータを更新するなど、ユーザに対して独自のサービスを提供する。

【００２８】また、図１に、図２における認証管理装置２１の内部構成を示す。図中、データベース管理部１は、認証管理装置又は認証管理システムの管理者の指示にしたがって仮パスワードデータベース７、ユーザ情報データベース８、認証手段データベース９、端末情報データベース１０の内容の管理を行う。

【００２９】仮パスワードデータベース７は、ユーザの認証情報を登録する時の認証に用いる仮パスワードに対応する情報が登録されるデータベースである。ユーザ情報データベース８は、ユーザ個人の認証情報に対応する情報が登録されるデータベースである。認証手段データベース９は、端末に入力される認証情報に応じて認証処

理を行う認証手段である認証管理装置２１内の認証パッケージに対応する情報が登録されるデータベースである。端末情報データベース１０は、認証手段を任意に組み合わせた認証条件に対応する情報が登録されるデータベースである。

【００３０】仮パスワード認証処理部２は、仮パスワードデータベース７を参照して仮パスワードによる認証を行う。ネットワーク通信部３は、ネットワーク２８を介して端末２２～２４との通信を行うと共に、端末２２～２４から受信したコマンドの種類を判別する。

【００３１】認証処理振り分け部４は、端末２２～２４から受信したコマンドが認証コマンドである場合、又は変更コマンドである場合に動作し、ユーザ情報データベース８でユーザの登録状況を確認し、認証手段データベース９で使用する認証パッケージを決定し、さらに端末情報データベース１０で認証条件を決定して、所定の認証パッケージに認証処理を振り分けると共に、各々の認証パッケージの認証結果に基づいて認証を行う。

【００３２】登録処理振り分け部５は、端末２２～２４から受信したコマンドが登録コマンドである場合に動作し、ユーザ情報データベース８でユーザの登録状況を確認し、仮パスワード認証処理部２にユーザの認証を依頼し、認証結果が真となった場合にユーザ情報データベース８に記載された認証パッケージにユーザの認証情報の登録を振り分ける。

【００３３】変更処理振り分け部６は、端末２２～２４から受信したコマンドが変更コマンドである場合に動作する。ユーザ情報データベース８でユーザの登録状況を確認し、認証手段データベース９で認証パッケージの情報を確認し、認証処理振り分け部４にユーザの認証を依頼する。認証結果が真となった場合に該当する認証パッケージにユーザの認証情報の変更を振り分ける。

【００３４】認証パッケージ１１～１３は、指紋照合、声紋照合、パスワード等、それぞれ異なる種類の認証を行うものであり、それぞれ、独自の登録処理部１４、変更処理部１５、認証処理部１６、認証情報データベース１７を持つ。登録処理部１４は、インタフェース装置２５～２７で採取されたユーザ個人の認証情報を独自の認証情報データベース１７に登録する。変更処理部１５は、独自の認証情報データベース１７に既に登録されている認証情報をインタフェース装置２５～２７で採取されたユーザの個人認証情報に変更する。認証処理部１６は、インタフェース装置２５～２７で採取されたユーザの個人認証情報を、独自の認証情報データベース１７に登録されている認証情報に基づいて認証する。

【００３５】図４に、仮パスワードデータベース７に登録される仮パスワードのデータ構造の一例を示す。Ｒ１１の列には、仮パスワードが登録される。Ｒ１２の列には、仮パスワード有効期限が登録される。Ｒ１３の列には、この仮パスワードを登録に用いるユーザ情報データベース８の項を示すポインタが登録される。

【００３６】このように、仮パスワードデータベース７は、少なくとも仮パスワードと共にその仮パスワードの有効期限が登録され、認証管理装置２１で管理される。

【００３７】図５に、ユーザ情報データベース８に登録されるユーザ個人の認証情報のデータ構造の一例を示す。Ｒ２１の列には、ユーザを一義に示すユーザＩＤが登録される。Ｒ２２～Ｒ２４の列には、Ｒ２１内のユーザＩＤに対応するユーザの認証手段毎の認証情報の登録状況が登録される。各Ｒ２２～Ｒ２４において、ｒ２１の列には、登録フラグが登録される。フラグ１は認証パッケージの認証情報が登録待ち状態であることを示し、フラグ０は登録済みであることを示す。ｒ２２の列には、認証情報を登録する際に用いる仮パスワードに対応するポインタ、又は認証情報が登録されている認証情報データベース内のポインタが登録される。ＮＵＬＬはユーザが該認証パッケージを使用しないことを示す。

【００３８】このように、ユーザ情報データベース８は、少なくともユーザ毎に複数の認証パッケージに対する登録状況が登録され、認証管理装置２１で管理される。

【００３９】図６に、認証手段データベース９に登録される認証パッケージの情報のデータ構造を示す。Ｒ３１の列には、認証パッケージ１１～１３を一義に示す識別子である認証手段ＩＤが登録される。Ｒ３２の列には、認証手段ＩＤの示す認証パッケージ１１～１３の認証処理部１６と対応するポインタが登録される。Ｒ３３の列には、認証手段ＩＤの示す認証パッケージ１１～１３の登録処理部１４と対応するポインタが登録される。Ｒ３４の列には、認証手段ＩＤの示す認証パッケージ１１～１３の変更処理部１５と対応するポインタが登録される。

【００４０】Ｒ３５の列には、一般の認証（通常の認証）を行うときに、認証処理部１６に渡されるしきい値が登録される。なお、ＮＵＬＬはしきい値がない場合を示す。Ｒ３６の列には、認証情報変更時の認証を行うときに、認証処理部１６に渡されるしきい値が登録される。なお、ＮＵＬＬはしきい値がない場合を示す。Ｒ３７の列には、Ｒ３５及びＲ３６以外で認証処理部１６に渡されるパラメタ値が登録される。なお、ＮＵＬＬはパラメタ値がない場合を示す。

【００４１】このように、認証手段データベース９は、少なくとも認証手段毎の一般認証時のしきい値と認証情報変更時のしきい値とを区別して登録され、認証管理装置２１で管理される。

【００４２】図７に、端末情報データベース１０に登録される認証条件のデータ構造を示す。Ｒ４１の列には、端末を一義に示す識別子である端末ＩＤが登録される。Ｒ４２の列には、端末毎に通常の認証に用いるの認証条件を示す一般認証式が登録される。Ｒ４３～Ｒ４４の列

には、それぞれ特定のサービスやアプリケーション専用の認証条件を示す特定認証式が登録される。

【００４３】このように、端末情報データベース１０は、少なくとも端末毎に通常の認証で用いる認証条件と特定のサービスやアプリケーションで用いる認証条件とを区別して登録され、認証管理装置２１で管理される。

【００４４】次に、動作について説明する。まず、新たな認証パッケージを認証管理装置２１に登録する際の動作について説明する。図８は、認証パッケージを登録する際の処理の流れを示すフローチャートである。

【００４５】管理者がデータベース管理部１に認証パッケージの追加を指示すると、処理がスタートする。まず、ＳＴＥＰ１で、データベース管理部１は、認証手段データベース９に新たな行を追加する。例えば、図６におけるＧ３３を追加し、Ｇ３３－Ｒ３１に登録する認証パッケージに対応する認証手段ＩＤを登録する。この例では“声紋”を登録する。

【００４６】ＳＴＥＰ２で、データベース管理部１は、続いてＧ３３－Ｒ３２、Ｇ３３－Ｒ３３、Ｇ３３－Ｒ３４のそれぞれに、認証パッケージ１１の認証処理部１６、登録処理部１４、変更処理部１５のポインタを登録する。

【００４７】ＳＴＥＰ３で、データベース管理部１は、さらにＧ３３－Ｒ３５に一般認証しきい値を登録する。例えば、しきい値は管理者によって指定された値を登録する。バイオメトリクスによる個人認証の場合、認証情報と登録されている情報がしきい値以上一致した場合、認証ＯＫとされる。そのため、しきい値が高いほど他人によるなり澄ましは難しくなるが、本人が拒否される確率も高くなる。

【００４８】ＳＴＥＰ４で、データベース管理部１は、さらにＧ３３－Ｒ３６に変更時認証しきい値を登録する。この値についても、例えば、管理者によって指定された値を登録する。このとき、一般認証しきい値と区別して、より高い値を登録することにより、通常の認証時のセキュリティ強度と認証情報変更時の認証時のセキュリティ強度とを区別することができる。

【００４９】ＳＴＥＰ５で、データベース管理部１は、さらにＧ３３－Ｒ３７にその他のパラメタを登録し、処理を終了する。なお、このパラメタ値は、認証実施時に、認証処理振り分け部１３が認証パッケージ１１の認証処理部１６にそのまま渡す値である。

【００５０】このように、管理者がデータベース管理部１に認証パッケージの追加を指示すると、データベース管理部１によって、登録する認証パッケージに対応する認証手段ＩＤが認証手段データベース９に登録され、認証関数Ｒ３２の項目、登録関数Ｒ３３の項目などが登録される。さらに、一般認証しきい値と変更時認証しきい値とを区別して、例えば、管理者によって指定されたしきい値がそれぞれ設定され、認証パッケージを認証管理装置２１に登録できる。

【００５１】次に、新たな端末を認証管理装置２１に登録する際の動作について説明する。図９は、端末を登録する際の処理の流れを示すフローチャートである。

【００５２】管理者がデータベース管理部１に端末の追加を指示すると、処理がスタートする。まず、ＳＴＥＰ６で、データベース管理部１は、端末情報データベース１０に新たな行を追加する。例えば、図７におけるＧ４５を追加し、Ｇ４５－Ｒ４１に登録する端末を一義に示す端末ＩＤを設定する。この端末ＩＤは、必ずしも１端末に１つ設定する必要はない。例えば、図３におけるパソコンＩ１１とＩ１２のように、同様の動作を行う端末については、グループとして１つの端末ＩＤを設定する。この例では“パソコン２”を設定する。

【００５３】ＳＴＥＰ７で、データベース管理部１は、続いてＧ４５－Ｒ４２に一般認証式を登録する。例えば、管理者によって指定された一般認証式を登録する。この一般認証式は、この端末において行われる通常の認証に対する認証条件を示す。また、一般認証式は、ＡＮＤ及びＯＲを用いて自由に設定可能としてもよい。例えば、Ｇ４１－Ｒ４２は、ユーザＩＤと指紋による認証か、又はＩＤカードでの認証を許すものである。

【００５４】ＳＴＥＰ８で、データベース管理部１は、さらにＧ４５－Ｒ４３～Ｒ４４に特定認証式を登録し、処理を終了する。この式についても、例えば、管理者によって指定された特定認証式を登録する。特定認証式は、特定のアプリケーションに対する認証で用いる認証式であり、“アプリケーションＩＤ＝認証式”の書式であらわす。アプリケーションＩＤは、端末内で認証を必要とするアプリケーションを一意に示す識別子である。また、特定認証式は、アプリケーション毎に複数設定可能であり、特定認証式が複数ある場合は左詰で登録し、すべての登録が終了したら、Ｇ４４－Ｒ４４のようにＮＵＬＬを登録する。

【００５５】右辺にＮＵＬＬを登録した場合は、そのアプリケーションＩＤの認証はすべてＮＧとなり、その端末でのアプリケーションの使用の禁止を示す。また、特定認証式は一般認証式と同様に、ＡＮＤ及びＯＲを用いて自由に設定可能としてもよい。こうして端末毎に、また、その端末内のアプリケーション毎に認証式を区別して登録する。

【００５６】このように、管理者がデータベース管理部１に端末の追加を指示すると、データベース管理部１によって、登録する端末に対応する端末ＩＤが端末情報データベース１０に登録される。さらに、例えば、管理者によって指定された認証手段を任意に組み合わせた認証条件である認証式が、端末毎、アプリケーション毎に区別されて、それぞれ一般認証式Ｒ４２の項目、特定認証式Ｒ４３の項目などに登録され、端末を認証管理装置２１に登録できる。

【００５７】次に、新たなユーザを認証管理装置２１に登録する際の動作について説明する。図１０は、ユーザを登録する際の処理の流れを示すフローチャートである。

【００５８】管理者がデータベース管理部１にユーザの追加を指示すると、処理がスタートする。まず、ＳＴＥＰ９で、データベース管理部１は、ユーザ情報データベース８に新たな行を追加する。例えば、図５におけるＧ２３を追加し、Ｇ２３－Ｒ２１にそのユーザを一義に示すユーザＩＤを登録する。この例では“Ｕｓｅｒ３”を登録する。

【００５９】ＳＴＥＰ１０で、データベース管理部１は、登録フラグを１に設定する。例えば、ユーザが使用する認証手段として指紋と声紋の登録を行う場合、指紋Ｒ２２の登録フラグＧ２３－ｒ２１と、声紋Ｒ２３の登録フラグＧ２３－ｒ２１を１に設定する。登録フラグはその列における認証手段の認証情報の登録状態を示すものであり、１は登録待ち状態を示し、０は登録済み状態を示す。

【００６０】ＳＴＥＰ１１で、データベース管理部１は、仮パスワードデータベース７に新たな行を追加する。例えば、図４におけるＧ１１を追加し、Ｇ１１－Ｒ１１にＳＴＥＰ１０で登録フラグに１を設定した認証情報に対する仮パスワードを登録する。

【００６１】ＳＴＥＰ１２で、さらにデータベース管理部１は、その仮パスワードに対応する有効期限をＧ１１－Ｒ１１に登録し、ＳＴＥＰ１３で、ユーザ情報データベースのＧ２３－Ｒ２２のポインタをＧ１１－Ｒ１３に登録する。

【００６２】ＳＴＥＰ１４で、仮パスワードのポインタをユーザ情報データベース８に登録する。例えば、Ｇ１１のポインタをＧ２３－ｒ２２に登録する。同様のＳＴＥＰ１１からＳＴＥＰ１４の処理を各列について行う。最後に、ＳＴＥＰ１５で、仮パスワードをユーザに通知し、処理を終了する。

【００６３】このように、管理者がデータベース管理部１にユーザの追加を指示すると、データベース管理部１によって、登録するユーザに対応するユーザＩＤがユーザ情報データベースに登録される。このときユーザＩＤは、仮パスワード及びその有効期限と関連付けられて登録され、ユーザに仮パスワードを通知すると共に、ユーザを認証管理装置２１に登録できる。

【００６４】次に、端末からのコマンドに対する認証管理装置２１の処理について説明する。端末から送信されるコマンドには、登録コマンド、変更コマンド、認証コマンドがある。図１１は、端末からのコマンドを認証管理装置２１が受信した際の処理の流れを示すフローチャートである。

【００６５】端末から発信されたコマンドは、ネットワーク２８を介して、ネットワーク通信部３に到達する。ネットワーク通信部３がコマンドを受信するとコマンドに対する処理がスタートする。

【００６６】ＳＴＥＰ１６で、ネットワーク通信部３は、受信したコマンドが登録コマンド、変更コマンド又は認証コマンドのどのコマンド種別であるかを判別する。判別結果が登録コマンドである場合は、同時に受信した端末ＩＤ、ユーザＩＤ、認証手段ＩＤ、認証情報、仮パスワードと共に、登録処理を登録処理振り分け部５に依頼し、ＳＴＥＰ１７に進む。

【００６７】判別結果が変更コマンドである場合は、同時に受信した端末ＩＤ、ユーザＩＤ、変更用の認証手段ＩＤと認証情報、認証用の認証手段ＩＤと認証情報と共に、変更処理を変更処理振り分け部６に依頼し、ＳＴＥＰ３０に進む。なお、認証用の認証手段ＩＤと認証情報は、端末から１組以上送信されるものとする。

【００６８】また、判別結果が認証コマンドである場合は、同時に受信した端末ＩＤ、ユーザＩＤ、認証手段ＩＤ、アプリケーションＩＤ、認証情報と共に、認証処理を認証処理振り分け部４に依頼し、ＳＴＥＰ４０に進む。なお、この時、ユーザＩＤとアプリケーションＩＤはなくともよい。また、認証手段ＩＤと認証情報は、１組以上送信されるものとする。

【００６９】まず、登録コマンドの場合について説明する。ＳＴＥＰ１７で、登録処理振り分け部５は、ユーザ情報データベース８を検索して、ユーザＩＤとマッチする行を探す。例えば、受信したユーザＩＤがＵｓｅｒ３の場合、図５においてＧ２３がマッチする。

【００７０】ＳＴＥＰ１８で、登録処理振り分け部５は、Ｇ２３－ｒ２１の登録フラグが１、かつＧ２３－ｒ２２のポインタがＮＵＬＬでないかを判定する。その結果、登録フラグが１で、ポインタがＮＵＬＬでない場合、すなわち、認証情報の登録待ち状態であり、かつ仮パスワードのポインタがＮＵＬＬでない場合は、ＳＴＥＰ１９に進む。それ以外の場合は、ＳＴＥＰ２４に進む。

【００７１】ＳＴＥＰ１９で、登録処理振り分け部５が仮パスワード認証処理部２にＧ２３－ｒ２２のポインタを渡して仮パスワードの認証を依頼すると、仮パスワード認証部２は、受信した仮パスワードとＧ１１－Ｒ１１を用いて仮パスワード認証を行い、仮パスワードを判定する。判定結果がＯＫの場合は、ＳＴＥＰ２０に進み、ＮＧの場合は、ＳＴＥＰ２４に進む。

【００７２】ＳＴＥＰ２０で、登録処理振り分け部５が認証手段データベース９から受信した認証手段ＩＤと一致する行の登録関数Ｒ３３のポインタを検索し、そのポインタ、受信したユーザＩＤ及び認証情報を用いて認証パッケージ１１の登録処理部１４に登録を依頼すると、登録処理部１４はその認証情報を認証パッケージ内の認証データベース１７に登録する。このとき、登録処理部１４は、リターン値として該当情報の認証情報データベ

ース１７内のポインタを登録処理振り分け部５に返す。
【００７３】ＳＴＥＰ２１で、登録処理振り分け部５の依頼を受けて仮パスワード認証処理部は、仮パスワードデータベース７の該当する行Ｇ１１を削除する。これにより、削除された仮パスワードは無効となり、使用不可能となる。
【００７４】ＳＴＥＰ２２で、登録処理振り分け部５は、登録処理部１４のリターン値をユーザ情報データベース８のＧ２３－ｒ２２に登録し、登録フラグＧ２３－ｒ２１を０に設定する。
【００７５】ＳＴＥＰ２３で、登録処理振り分け部５は、正常通知をネットワーク通信部３を介して端末ＩＤに対応する端末に送信し、登録コマンドに対する処理を終了する。
【００７６】一方、ＳＴＥＰ１８でＮ、又はＳＴＥＰ１９でＮＧの場合は、ＳＴＥＰ２４で、登録処理振り分け部５は、エラーログを記録し、異常通知をネットワーク通信部３を介して端末ＩＤに対応する端末に送信し、登録コマンドに対する処理を終了する。
【００７７】次に、変更コマンドの場合について説明する。ＳＴＥＰ３０で、変更処理振り分け部６は、ユーザＩＤ、認証用の認証手段ＩＤと認証情報をもって、認証処理振り分け部４に認証依頼をする。
【００７８】ＳＴＥＰ３１で、変更処理振り分け部６は、認証処理振り分け部４による認証結果を確認する。認証結果がＯＫの場合はＳＴＥＰ３２に進み、認証結果がＮＧの場合はＳＴＥＰ３６に進む。
【００７９】ＳＴＥＰ３２で、変更処理振り分け部６は、ユーザ情報データベース８を検索して、ユーザＩＤに該当する認証情報のポインタの行を検索する。さらに、ＳＴＥＰ３３で、変更処理振り分け部６は、認証手段データベース９を検索して、変更用の認証手段ＩＤに該当する変更関数の行を検索する。
【００８０】ＳＴＥＰ３４で、変更処理振り分け部６は、変更関数ポインタＲ３３、認証情報のポインタｒ２２及び変更用の認証情報をもって変更処理部１４に認証情報の変更を依頼する。これを受けて変更処理部１４は、認証情報データベース１７内のユーザの認証情報を変更用の認証情報に書き換える。
【００８１】ＳＴＥＰ３５で、変更処理振り分け部６は、正常通知をネットワーク通信部３を介して端末ＩＤに対応する端末に送信し、変更コマンドに対する処理を終了する。
【００８２】一方、ＳＴＥＰ３１でＮＧの場合は、ＳＴＥＰ３６で、変更処理振り分け部６は、エラーログを記録し、異常通知をネットワーク通信部３を介して端末ＩＤに対応する端末に送信し、変更コマンドに対する処理を終了する。
【００８３】次に、認証コマンドの場合について説明する。ＳＴＥＰ４０で、認証処理振り分け部４は、認証処理を行う。この詳細は、図１２を使って、別途説明する。
【００８４】ＳＴＥＰ４１で、認証結果を確認する。認証結果がＯＫならＳＴＥＰ４２で、認証処理振り分け部４は、正常通知と共に認証ＯＫをネットワーク通信部３を介して端末ＩＤに対応する端末に送信し、認証コマンドに対する処理を終了する。
【００８５】一方、ＳＴＥＰ４１で認証結果がＮＧならＳＴＥＰ４３で、認証処理振り分け部４は、エラーログを記録し、異常通知をネットワーク通信部３を介して端末ＩＤに対応する端末に送信し、認証コマンドに対する処理を終了する。
【００８６】次に、ＳＴＥＰ４０の認証処理の詳細を説明する。図１２は、認証処理の詳細な処理の流れを示すフローチャートである。まず、ＳＴＥＰ５０で、認証処理振り分け部４は、端末情報データベース１０を検索して受信した端末ＩＤと一致する行を検索する。
【００８７】ＳＴＥＰ５１で、認証処理振り分け部４は、アプリケーションＩＤから該当する認証式を決定する。アプリケーションＩＤが指定されない場合は、一般認証式とする。ＳＴＥＰ５２で、認証式にマッチする認証ＩＤと認証情報を端末から受信しているかどうかをチェックする。ＯＫの場合はＳＴＥＰ５３に進み、ＮＧの場合はＳＴＥＰ６２に進む。
【００８８】ＳＴＥＰ５３で、認証処理振り分け部４は、認証手段データベース９を検索して受信した認証手段ＩＤと一致する行を検索し、ＳＴＥＰ５４で、コマンド種別を判別する。認証コマンドの場合はＳＴＥＰ５５で、一般認証しきい値を選択し、変更コマンドの場合はＳＴＥＰ５６で、変更時認証しきい値を選択する。
【００８９】ＳＴＥＰ５７で、認証処理振り分け部４は、ユーザ情報データベースをユーザＩＤと認証手段ＩＤで検索し、該当するポインタｒ２２を検索する。ユーザＩＤが指定されていない場合は、ポインタ値はＮＵＬＬとする。
【００９０】ＳＴＥＰ５８で、認証処理振り分け部４は、ＳＴＥＰ５５～５７で検索したしきい値とポインタ値で、認証関数ポインタＲ３２を用いて該当する認証パッケージ１１の認証処理部１６をコールする（認証処理を依頼する）。これを受けて、認証処理部１６は認証を実施し、結果を認証処理振り分け部４に返す。
【００９１】ＳＴＥＰ５９で、認証処理振り分け部４は、認証処理部１６の認証結果を確認する。認証結果がＯＫの場合はＳＴＥＰ６０に進み、認証結果がＮＧの場合はＳＴＥＰ６２に進む。
【００９２】さらに、ＳＴＥＰ６０で、認証処理振り分け部４は、認証式が成立したか否かを確認する。認証式が成立しない場合は、成立するまでＳＴＥＰ５３から次の認証手段ＩＤと認証情報について認証処理を繰り返す。一方、認証式が成立する場合は、ＳＴＥＰ６１に進

み、認証ＯＫとして、認証処理を終了する。

【００９３】また、ＳＴＥＰ５２又はＳＴＥＰ５９でＮＧの場合は、ＳＴＥＰ６２に進み、認証ＮＧとして、認証処理を終了する。

【００９４】このように、ユーザが端末を用いてサービスを受ける場合、ネットワーク通信部３によってコマンドが判別され、そのコマンドに応じて処理がなされる。例えば、ユーザが認証情報を登録する際は、ネットワーク通信部３によって登録コマンドが判別され、登録処理振り分け部５の指示によって、仮パスワードによる認証がなされた後、所定の認証パッケージにユーザの認証情報が登録されて、ユーザの認証情報を登録することができる。また同時に、仮パスワードデータベース７から使用した仮パスワードが削除され、以降その仮パスワードは使用できなくなる。

【００９５】また、ユーザが認証情報を変更する際は、ネットワーク通信部３によって変更コマンドが判別され、変更処理振り分け部６の指示によって、所定の認証パッケージの認証情報が変更される。この時、認証手段データベース１０に登録されたしきい値に従って、一般の認証より厳しい認証がなされて、ユーザの認証情報を変更することができる。

【００９６】また、ユーザが認証を依頼する際は、ネットワーク通信部３によって認証コマンドが判定され、認証処理振り分け部４の指示によって、認証手段データベース１０に登録されたしきい値に従って、認証情報変更時の認証より緩い認証がなされて、個人の判別（認証）をすることができる。

【００９７】次に、仮パスワード認証処理部２における仮パスワードの有効期限確認の際の処理について説明する。図１３は、仮パスワードの有効期限確認の際の仮パスワード認証処理部２の処理の流れを示すフローチャートである。

【００９８】一定時間毎に自動的に処理がスタートする。まず、ＳＴＥＰ７０で、仮パスワード認証処理部２は、仮パスワードのポインタに基づいて仮パスワードデータベース７の有効期限Ｒ１１を検索し、その有効期限を確認する。その結果、有効期限内であるときは、そのまま処理を終了する。

【００９９】一方、有効期限を過ぎている場合は、ＳＴＥＰ７２に進み、仮パスワード認証処理部２が登録処理振り分け部５に対して仮パスワードの認証ＮＧを通知すると、登録処理振り分け部５は、ユーザ情報データベース８内のユーザ情報データポインタＲ１３が示すポインタ（ｒ２２）をＮＵＬＬに変える。

【０１００】また、ＳＴＥＰ７２で、仮パスワード認証処理部２は、有効期限を過ぎた仮パスワードデータベース７のその行を削除し、処理を終了する。仮パスワード認証処理部２及び登録処理振り分け部は、以上の処理をすべての行について、定期的に実行し、確認する。

【０１０１】このように、認証情報を登録する際に用いる仮パスワードは、仮パスワードデータベース７に登録された有効期限によって管理され、有効期限が切れると自動的に使用できなくなる。

【０１０２】以上のように、本実施の形態に係る認証管理装置によれば、端末毎に通常の認証で用いる一般用の認証条件と、特定のサービスやアプリケーションで用いる認証条件とを区別して、複数の認証手段を任意に組み合わせた認証条件が登録される端末情報データベースを備えることにより、様々なサービスを提供する複数の端末やアプリケーションによる異なる認証方式を同一の認証管理装置を使用して一括して設定でき、管理者の作業を容易にできると共に、管理者が全てのシステムやアプリケーションに対して統一したセキュリティ・ポリシーのもとに認証条件を設定し、管理できる。

【０１０３】また、ユーザの認証情報を登録する際に参照される仮パスワードとその仮パスワードの有効期限とを関連付けて登録される仮パスワードデータベースを備え、有効期限に応じて又は認証情報の登録に応じて仮パスワードデーターベースから仮パスワードを削除することにより、例えば、ユーザが何らかの理由で長時間認証情報の登録を行わないときに自動的に登録が不可能となり、不正な認証情報の登録を回避でき、高度なセキュリティを必要とする場合に適用できる。

【０１０４】また、認証手段毎に通常の認証で用いる一般認証時のしきい値と、認証情報を変更する際に用いる認証情報変更時のしきい値とを区別して登録できる認証手段データベースを備え、通常の認証には一般認証時のしきい値を用い、認証情報を変更する際には認証情報変更時のしきい値を用いて認証処理することにより、認証情報変更時の認証を通常の認証より厳しくできる。例えば、よく似た他人によるバイオメトリクスの認証情報の変更を困難にでき、高度なセキュリティを必要とする場合に適用できる。

【０１０５】また、認証情報のうち少なくとも一つはバイオメトリクスの認証情報を用いることにより、より厳密に個人認証することができ、高度なセキュリティを必要とする場合に適用できる。

【０１０６】さらにまた、本実施の形態に係る認証管理システムによれば、端末毎に通常の認証で用いる一般用の認証条件と、特定のサービスやアプリケーションで用いる認証条件とを区別して、複数の認証手段を任意に組み合わせた認証条件が登録される端末情報データベースを備える認証管理装置を有することにより、様々なサービスを提供する複数の端末やアプリケーションによる異なる認証方式を同一の認証管理装置を使用して一括して設定でき、管理者の作業を容易にできると共に、管理者が全てのシステムやアプリケーションに対して統一したセキュリティ・ポリシーのもとに認証条件を設定し、管理できる。

【0107】また、ユーザの認証情報を登録する際に参照される仮パスワードとその仮パスワードの有効期限とを関連付けて登録される仮パスワードデータベースを備え、有効期限に応じて又は認証情報の登録に応じて仮パスワードデーターベースから仮パスワードを削除する認証管理装置を有することにより、例えば、ユーザが何らかの理由で長時間認証情報の登録を行わないときに自動的に登録が不可能となり、不正な認証情報の登録を回避でき、高度なセキュリティを必要とする場合に適用できる。

【0108】また、認証手段毎に通常の認証で用いる一般認証時のしきい値と、認証情報を変更する際に用いる認証情報変更時のしきい値とを区別して登録できる認証手段データベースを備え、通常の認証には一般認証時のしきい値を用い、認証情報を変更する際には認証情報変更時のしきい値を用いて認証処理する認証管理装置を有することにより、認証情報変更時の認証を通常の認証より厳しくできる。例えば、よく似た他人によるバイオメトリクスの認証情報の変更を困難にでき、高度なセキュリティを必要とする場合に適用できる。

【0109】また、認証情報のうち少なくとも一つはバイオメトリクスの認証情報を用いることにより、より厳密に個人認証することができ、高度なセキュリティを必要とする場合に適用できる。

【0110】なお、本実施の形態では、仮パスワードは有効期限内は常に有効である場合について説明したが、さらに、有効となる条件として時刻や端末の条件を加えてもよい。これにより、さらにセキュリティを向上できる。例えば、有効条件として、特定時刻の8時から17時と特定端末のドア制御とを追加することにより、認証情報の登録は、管理者が監視できる時刻の8時から17時にドア制御の端末からしか行えなくなる。

【0111】また、本実施の形態では、認証のしきい値のみで認証情報変更時の認証と通常の認証とを区別する場合について説明したが、さらに、認証処理を実施する時刻やコマンドを発行する端末の条件を付けてもよい。これにより、さらにセキュリティを向上できる。例えば、認証情報の変更は、8時から17時までに特定の端末からしか行えないようにすることができる。

【0112】また、本実施の形態では、認証情報の登録には常に仮パスワードを用いる場合について説明したが、既に登録されている別の種類の認証情報がある場合は、認証情報の変更と同じように、その認証情報で変更時認証用しきい値を用いて認証するようにしてもよい。これにより、仮パスワードを使用する機会を減少でき、よりセキュリティを向上できる。また、既に登録されている認証情報を用いて別の認証情報を登録する際の有効期限を設けてもよく、本実施の形態と同様の効果が得られる。例えば、新たに声紋の認証情報を登録する際に、既に登録されている指紋の認証情報を用いて認証して声紋の認証情報を登録する。また、指紋の認証情報に対して、登録のための認証に用いる場合の有効期限を設ける。

【0113】

【発明の効果】以上のように、本発明の認証管理装置によれば、認証手段を任意に組み合わせた認証条件に対応する情報が登録される端末情報データベースを備えることにより、異なる認証方式を同一の認証管理装置を使用して一括して設定でき、管理者の作業を容易にできると共に、管理者が全ての認証方式に対して統一したセキュリティ・ポリシーのもとに認証条件を設定し、管理できる。

【0114】また、本発明の認証管理装置によれば、ユーザの認証情報を登録する際に参照される仮パスワードとその仮パスワードの有効期限とを関連付けて登録される仮パスワードデータベースを備え、有効期限に応じて又は認証情報の登録に応じて仮パスワードデーターベースから仮パスワードを削除することにより、不正な認証情報の登録を回避でき、高度なセキュリティを必要とする場合に適用できる。

【0115】また、本発明の認証管理装置によれば、認証手段毎に通常の認証で用いる一般認証時のしきい値と、認証情報を変更する際に用いる認証情報変更時のしきい値とを区別して登録できる認証手段データベースを備え、通常の認証には一般認証時のしきい値を用い、認証情報を変更する際には認証情報変更時のしきい値を用いて認証処理することにより、例えば、認証情報変更時の認証を通常の認証より厳しくでき、高度なセキュリティを必要とする場合に適用できる。

【0116】また、本発明の認証管理装置によれば、認証情報の少なくとも一つはバイオメトリクスの認証情報であることにより、より厳密に個人認証することができ、高度なセキュリティを必要とする場合に適用できる。

【0117】さらにまた、本実施の認証管理システムによれば、認証手段を任意に組み合わせた認証条件に対応する情報が登録される端末情報データベースを備える認証管理装置を有することにより、異なる認証方式を同一の認証管理装置を使用して一括して設定でき、管理者の作業を容易にできると共に、管理者が全ての認証方式に対して統一したセキュリティ・ポリシーのもとに認証条件を設定し、管理できる。

【0118】また、本発明の認証管理装置システムによれば、ユーザの認証情報を登録する際に参照される仮パスワードとその仮パスワードの有効期限とを関連付けて登録される仮パスワードデータベースを備え、有効期限に応じて又は認証情報の登録に応じて仮パスワードデーターベースから仮パスワードを削除する認証管理装置を有することにより、不正な認証情報の登録を回避でき、高度なセキュリティを必要とする場合に適用できる。

【0119】また、本発明の認証管理装置システムによれば、認証手段毎に通常の認証で用いる一般認証時のしきい値と、認証情報を変更する際に用いる認証情報変更時のしきい値とを区別して登録できる認証手段データベースを備え、通常の認証には一般認証時のしきい値を用い、認証情報を変更する際には認証情報変更時のしきい値を用いて認証処理する認証管理装置を有することにより、例えば、認証情報変更時の認証を通常の認証より厳しくでき、高度なセキュリティを必要とする場合に適用できる。

【0120】また、本発明の認証管理装置システムによれば、認証情報の少なくとも一つはバイオメトリクスの認証情報であることにより、より厳密に個人認証することができ、高度なセキュリティを必要とする場合に適用できる。

【図面の簡単な説明】

【図1】　この発明の実施の形態1における認証管理装置の構成を示すブロック図。

【図2】　この発明の実施の形態1における認証管理システムのシステム構成を示すブロック図。

【図3】　この発明の実施の形態1における認証管理システムの具体的なシステム構成を示すブロック図。

【図4】　この発明における仮パスワードデータベースのデータ構成を示す図表。

【図5】　この発明のユーザ情報データベースのデータ構成を示す図表。

【図6】　この発明の認証手段データベースのデータ構成を示す図表。

【図7】　この発明の端末情報データベースのデータ構成を示す図表。

【図8】　この発明の認証パッケージの登録手順を示すフローチャート。

【図9】　この発明の端末の登録手順を示すフローチャート。

【図10】　この発明のユーザの登録手順を示すフローチャート。

【図11】　この発明の端末からのコマンドに対する処理手順を示すフローチャート。

【図12】　この発明の認証処理の処理手順を示すフローチャート。

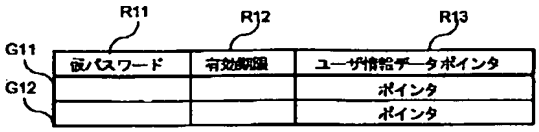
【図13】　この発明の仮パスワードの有効期限の確認処理の処理手順を示すフローチャート。

【図14】　従来の認証機能を備えたサービス・サーバのシステム構成を示すブロック図。

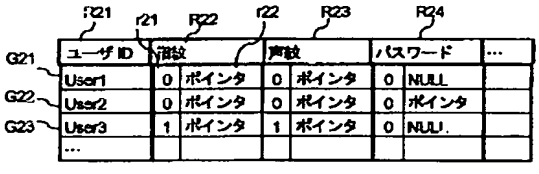
【符号の説明】

1　データベース管理部　　2　仮パスワード認証処理部
3　ネットワーク通信部　　4　認証処理振り分け部
5　登録処理振り分け部　　6　変更処理振り分け部
7　仮パスワードデータベース　　8　ユーザ情報データベース
9　認証手段データベース　　10　端末情報データベース
11～13　認証パッケージ　　14　登録処理部
15　変更処理部　　16　認証処理部
17　認証情報データベース　　21　認証管理装置
22～24　端末インタフェース装置　　25～27
28　ネットワーク　　A1　認証管理装置
C1　出退勤管理装置　　C2、C3　ドア制御装置
C4　勤怠管理装置　　C5　メールサーバ
I1　テンキーパット　　I2～I6　指紋取得装置
I7～I9　ICカードリーダ　　I10　声紋取得装置
I11～I15　パソコン　　31　サービス処理部
32　認証処理部　　33　認証情報データベース
34　登録サービス処理部

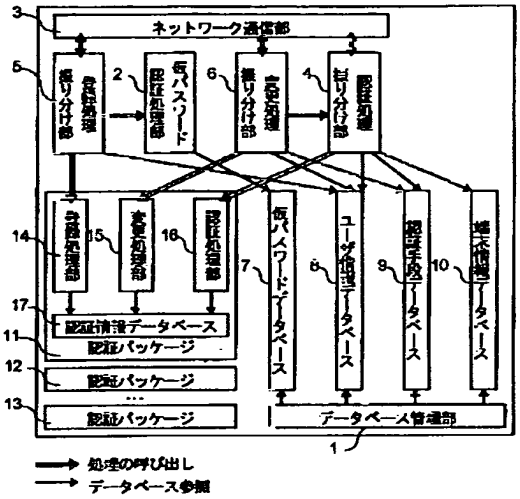
【図4】



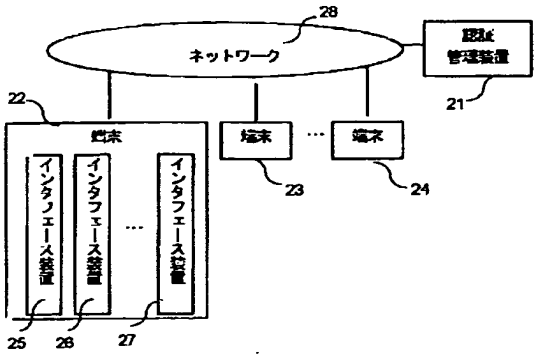
【図5】



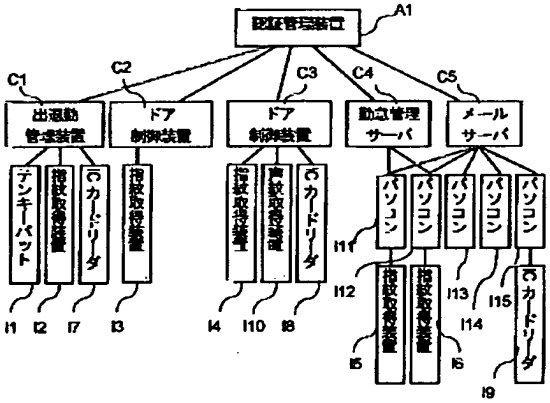
【図１】



【図２】



【図３】



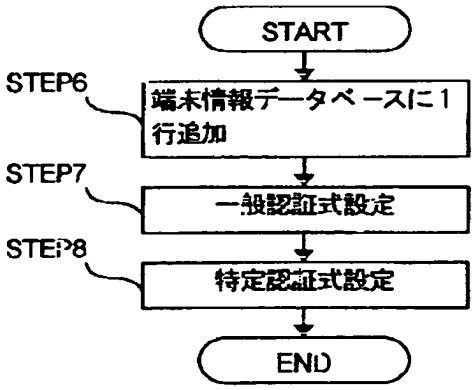
【図６】

	R31 認証手段ID	R32 認証関数	R33 登録関数	R34 変更関数	R35 一般認証しきい値	R36 変更時認証しきい値	R37 その他パラメタ
G31	パスワード	ポインタ	ポインタ	ポインタ	NULL	NULL	NULL
G32	指紋	ポインタ	ポインタ	ポインタ	値	値	値
G33	声紋	ポインタ	ポインタ	ポインタ	値	値	NULL
…							

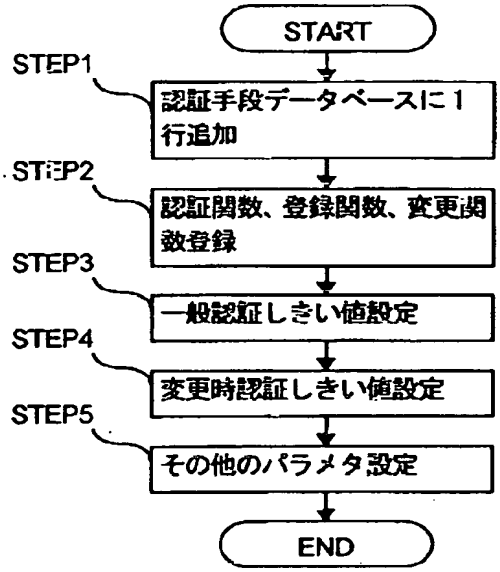
【図７】

	R41 端末ID	R42 一般認証式	R43 特定認証式１	R44 特定認証式２	…
G41	出退勤管理装置	(ユーザID＊指紋)＋ICカード	NULL		
G42	ドア制御装置１	指紋	NULL		
G43	ドア制御装置２	(指紋＊ICカード)＋(声紋＊ICカード)	NULL		
G44	パソコン１	ユーザID＊パスワード	勤怠管理＝ユーザID＊指紋	NULL	
G45	パソコン２	ICカード＊パスワード	勤怠管理＝NULL	NULL	
…					

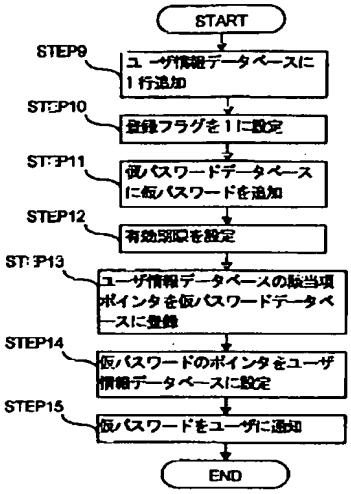
【図９】



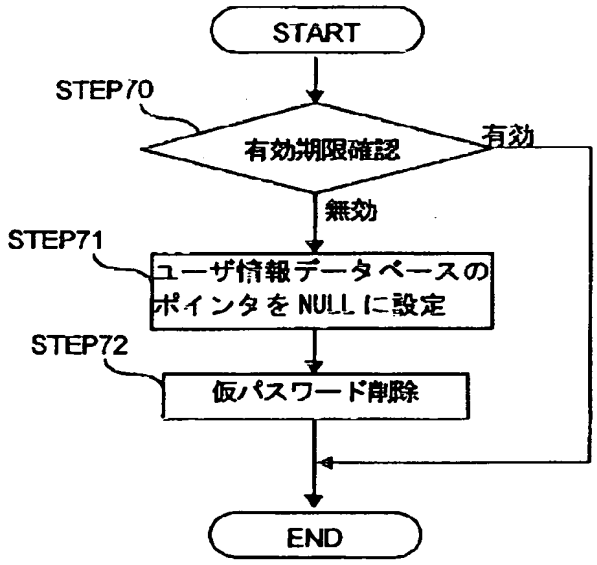
【図８】



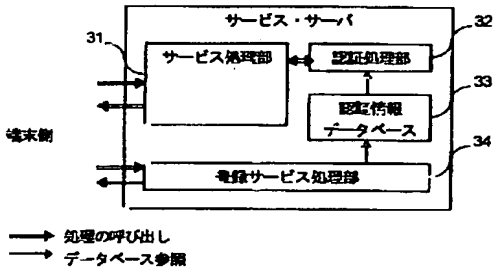
【図１０】



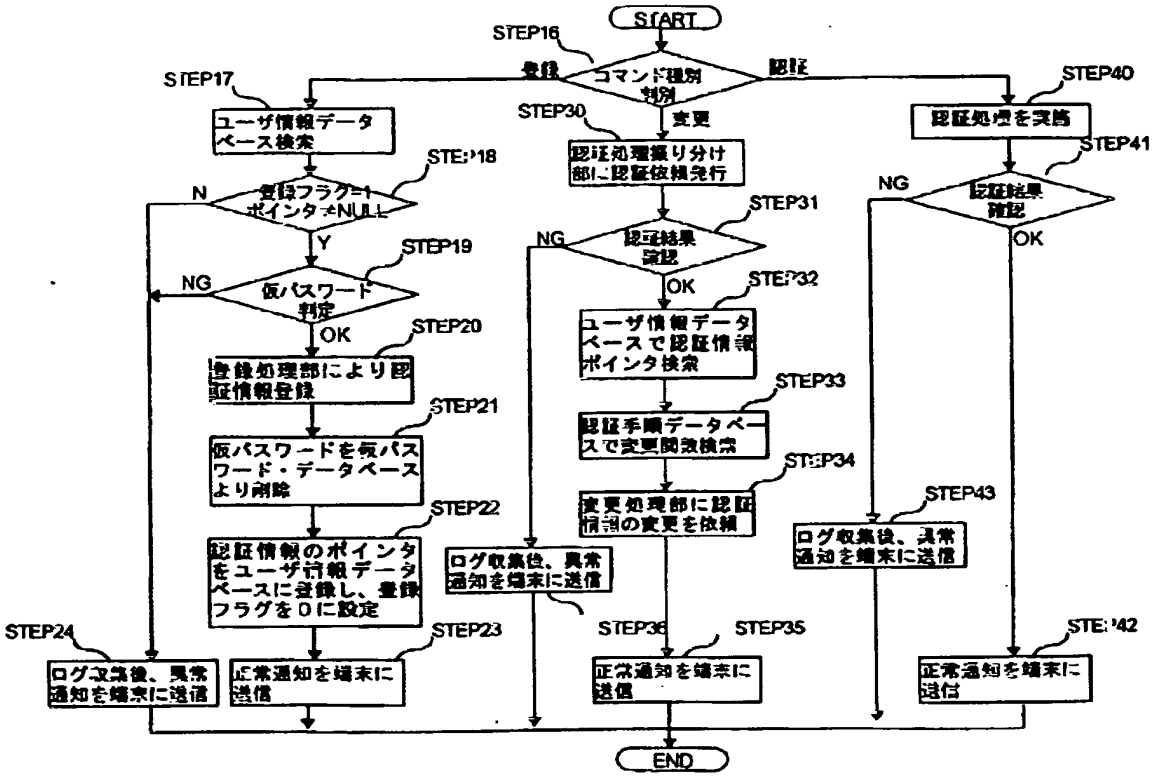
【図１３】



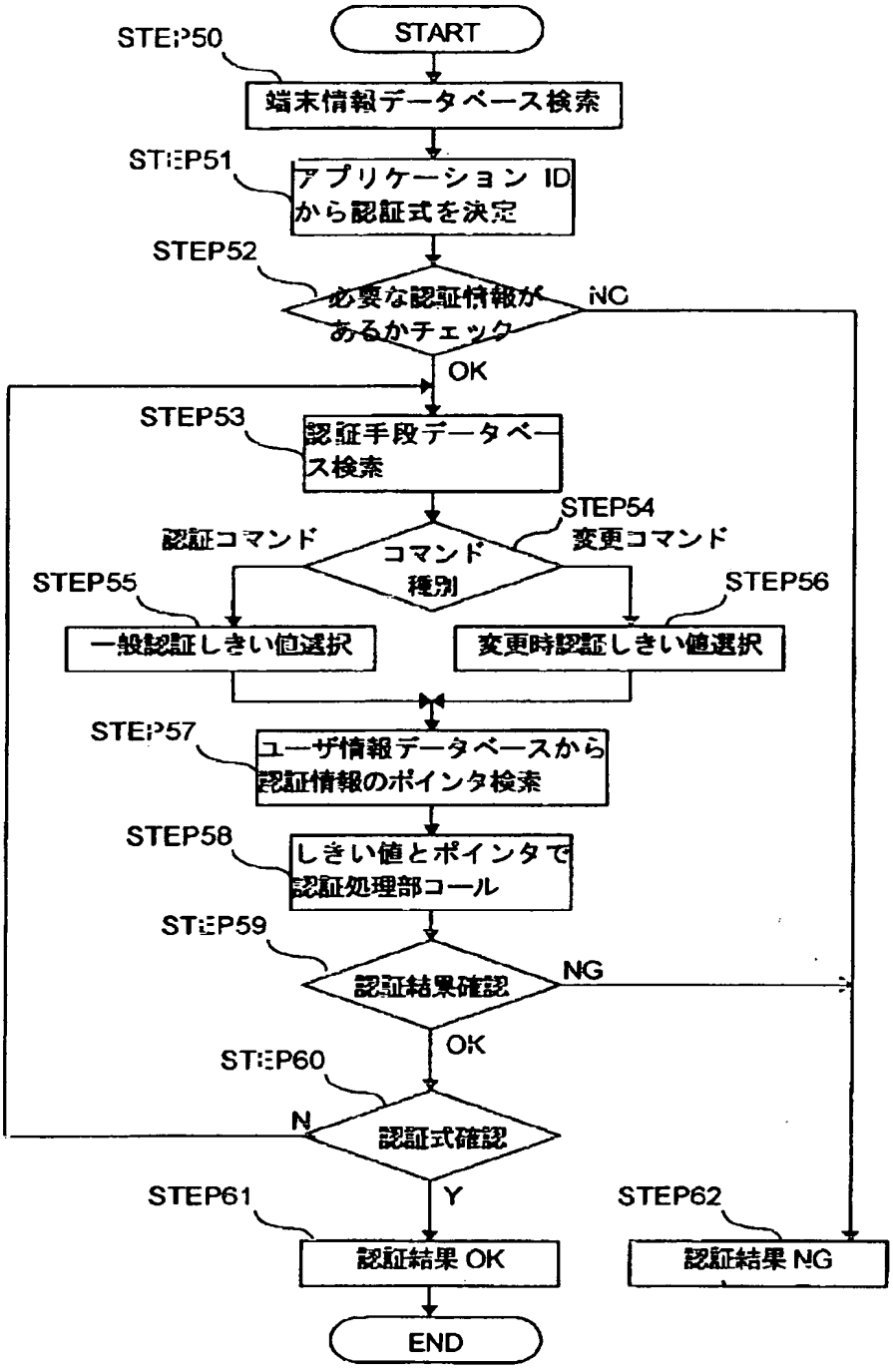
【図１４】



【図11】


START
STEP16
コマンド種別判別
登録
変更
認証
STEP17
ユーザ情報データベース検索
STEP30
認証処理振り分け部に認証依頼発行
STEP40
認証処理を実施
STEP18
登録フラグ=1 ポインタ≠NULL
N
Y
STEP31
認証結果確認
NG
OK
STEP41
認証結果確認
NG
OK
STEP19
仮パスワード判定
NG
OK
STEP32
ユーザ情報データベースで認証情報ポインタ検索
STEP20
登録処理部により認証情報登録
STEP33
認証手順データベースで変更関数検索
STEP21
仮パスワードを仮パスワード・データベースより削除
STEP34
変更処理部に認証情報の変更を依頼
STEP43
ログ収集後、異常通知を端末に送信
STEP22
認証情報のポインタをユーザ情報データベースに登録し、登録フラグを0に設定
ログ収集後、異常通知を端末に送信
STEP24
ログ収集後、異常通知を端末に送信
STEP23
正常通知を端末に送信
STEP36
STEP35
正常通知を端末に送信
STEP42
正常通知を端末に送信
END

【図12】


START
STEP50
端末情報データベース検索
STEP51
アプリケーション ID から認証式を決定
STEP52
必要な認証情報があるかチェック
NG
OK
STEP53
認証手段データベース検索
STEP54
認証コマンド
コマンド種別
変更コマンド
STEP55
STEP56
一般認証しきい値選択
変更時認証しきい値選択
STEP57
ユーザ情報データベースから認証情報のポインタ検索
STEP58
しきい値とポインタで認証処理部コール
STEP59
認証結果確認
NG
OK
STEP60
N
認証式確認
STEP61
Y
STEP62
認証結果 OK
認証結果 NG
END

フロントページの続き

(72)発明者　馬場　義昌
東京都千代田区丸の内二丁目２番３号　三
菱電機株式会社内